UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

ROYAL TRUCK & TRAILER SALES AND SERVICE, INC.,
Plaintiff,

v.

MIKE KRAFT; and KELLY MATTHEWS A/K/A/ KELLY SCHLIMMER,
Defendants.

Case No. 3:18-cv-10986-RHC-EAS
Hon. Robert H. Cleland
Mag. Elizabeth A. Stafford

KOTZ SANGSTER WYSOCKI P.C.
By: Anthony M. Sciara (P75778)
Christopher A. Ferlito (P80574)
Counsel for Royal Truck & Trailer
400 Renaissance Center
Suite 3400
Detroit, Michigan 48243
313-259-8300
asciara@kotzsangster.com
cferlito@kotzsangster.com

VARNUM LLP
By: Richard T. Hewlett (P41271)
Salvatore J. Vitale (P75449)
Counsel for Kraft and Matthews
39500 High Pointe Boulevard
Suite 350
Novi, Michigan 48375
248-567-7400
rthewlett@varnumlaw.com
sjvitale@varnumlaw.com

PLAINTIFF'S RESPONSE IN OPPOSITION TO DEFENDANTS' MOTION TO DISMISS UNDER RULE 12(B)(6) FOR FAILURE TO STATE A CLAIM UPON WHICH RELIEF CAN BE GRANTED AND UNDER RULE 12(B)(1) FOR WANT OF SUBJECT MATTER JURISDICTION

Now comes Plaintiff Royal Truck & Trailer Sales and Service, Inc., by its counsel, Kotz Sangster Wysocki P.C., in accordance with Federal Rule of Civil Procedure 12, and for its Response in Opposition to Defendants Mike Kraft's and Kelly Matthews a/k/a Kelly Schlimmer's Motion to Dismiss Under Rule 12(b)(6) for Failure to State a Claim and Under Rule 12(b)(1) for Want of Subject Matter Jurisdiction, states:

WHEREFORE, Plaintiff Royal Truck & Trailer Sales and Service, Inc. respectfully requests that, in accordance with Federal Rule of Civil Procedure 12, and for the reasons stated in its brief in support of this response, this Court deny Defendants Mike Kraft's and Kelly Matthews a/k/a Kelly Schlimmer's Motion to Dismiss Under Rule 12(b)(6) for Failure to State a Claim and Under Rule 12(b)(1) for Want of Subject Matter Jurisdiction.

Respectfully submitted,
KOTZ SANGSTER WYSOCKI P.C.

Dated: May 8, 2018 By: /s/ Anthony M. Sciara

Anthony M. Sciara (P75778)
Christopher A. Ferlito (P80574)
Counsel for Royal Truck & Trailer

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

ROYAL TRUCK & TRAILER SALES AND SERVICE, INC.,
Plaintiff,

v.

MIKE KRAFT; and KELLY MATTHEWS A/K/A/ KELLY SCHLIMMER,
Defendants.

Case No. 3:18-cv-10986-RHC-EAS
Hon. Robert H. Cleland
Mag. Elizabeth A. Stafford

KOTZ SANGSTER WYSOCKI P.C.
By: Anthony M. Sciara (P75778)
Christopher A. Ferlito (P80574)
Counsel for Royal Truck & Trailer
400 Renaissance Center
Suite 3400
Detroit, Michigan 48243
313-259-8300
asciara@kotzsangster.com
cferlito@kotzsangster.com

VARNUM LLP
By: Richard T. Hewlett (P41271)
Salvatore J. Vitale (P75449)
Counsel for Kraft and Matthews
39500 High Pointe Boulevard
Suite 350
Novi, Michigan 48375
248-567-7400
rthewlett@varnumlaw.com
sjvitale@varnumlaw.com

PLAINTIFF'S BRIEF IN SUPPORT OF ITS RESPONSE IN OPPOSITION TO DEFENDANTS' MOTION TO DISMISS UNDER RULE 12(B)(6) FOR FAILURE TO STATE A CLAIM UPON WHICH RELIEF CAN BE GRANTED AND UNDER RULE 12(B)(1) FOR WANT OF SUBJECT MATTER JURISDICTION

Now comes Plaintiff Royal Truck & Trailer Sales and Service, Inc. ("Royal"), by its counsel, Kotz Sangster Wysocki P.C., in accordance with Federal Rule of Civil Procedure 12, and for its Brief in Support of Its Response to Defendants Mike Kraft's ("Mike's") and Kelly Matthews a/k/a Kelly Schlimmer's ("Kelly's") (collectively "Defendants'") Motion to Dismiss Under Rule 12(b)(6) for Failure to State a Claim and Under Rule 12(b)(1) for Want of Subject Matter Jurisdiction, states:

QUESTIONS PRESENTED

A. Should the motion be summarily denied because Defendants failed to comply with Local Rule 7.1(a)(1)(2)?

Royal: Yes.
Defendants: No.

B. Do Counts I and II of the First Amended Complaint state claims upon which relief can be granted?

Royal: Yes.
Defendants: No.

1. Is the United States Court of Appeals for the Sixth Circuit likely to adopt, and should this Court follow, the broader approach (of the Circuit Split) taken by the First, Fifth, Seventh, Eighth, and Eleventh Circuits to interpreting the phrase "exceeds authorized access" under the Computer Fraud and Abuse Act?

Royal: Yes.
Defendants: No.

2. Do Counts I and II of the First Amended Complaint properly state claims that Defendants violated the Computer Fraud and Abuse Act because they exceeded their authorized access to company owned computers and cellular phones by using them in violation of company policies?

Royal:	Yes.
Defendants:	No.

CONTROLLING OR MOST APPROPRIATE LEGAL AUTHORITIES

"Broad" Approach

A. *E.F. Cultural Travel BV, EF v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001)

B. *International Airport Centers, L.L.C. v. Citrin*, 440 F.3d 418 (7th Cir. 2006)

C. *U.S. v. John*, 597 F.3d 263 (5th Cir. 2010)

D. *U.S. v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010)

E. *U.S. v. Teague*, 646 F.3d 1119 (8th Cir. 2011)

F. *American Furukawa, Inc. v. Hossain*, 103 F. Supp. 3d 864 (E.D. Mich. May 6, 2015)

"Narrow" Approach

G. *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009)

H. *U.S. v. Nosal*, 676 F.3d 854 (9th Cir. 2011)

I. *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012)

J. *U.S. v. Valle*, 807 F.3d 508 (2nd Cir. 2015)

K. *Ajuba Intern., L.L.C. v. Saharia*, 871 F. Supp. 2d 671 (E.D. Mich. May 14, 2012)

Sixth Circuit

L. *Pulte Homes, Inc. v. Laborers' International Union of North America*, 648 F.3d 295 (6th Cir. 2011)

Supreme Court

M. *Mussachio v. U.S.*, 136 S. Ct. 709 (2016)

TABLE OF CONTENTS

INDEX OF AUTHORITIES

CASES

OTHER AUTHORITIES

INTRODUCTION

On April 17, 2018, Defendants filed a combined Motion to Dismiss Under Rule 12(b)(6) for Failure to State a Claim and Under Rule 12(b)(1) for Want of Subject Matter Jurisdiction ("Motion"). (See ECF Doc. No. 11). The Motion asks this Court to dismiss Counts I and II of the First Amended Complaint ("Complaint") for failure to state a claim. (Id.). Counts I and II of the Complaint generally allege Defendants violated the CFAA when they exceeded their authorized access to company owned computers and cellular phones by using them in violation of company policies. (See ECF Doc. No. 8). According to Defendants, because Counts I and II of the Complaint are supposedly deficient, the entire nine count Complaint is nothing more than a "frivolous" product of "unclean hands and dubious intentions," which is designed only to "send a message" to other employees that "'[i]f you leave, we will drag you into federal court and attempt to make an example out of you.'" (ECF Doc. No. 11, at p. 4). This is obvious, Defendants conclude, because "this district's interpretation of the clear and unambiguous language of the CFAA … has been applied repeatedly and consistently[:] … [e]ven if an employee misappropriates or otherwise misuses confidential information, there is no violation of the CFAA unless the employee did not have access to that information in the first place." (Id.).

Defendants' invective is irrelevant and unfortunate. But Defendants' suggestion there is unanimity among courts concerning application of the CFAA is misleading (at best). Indeed, even the district court decisions relied upon heavily by Defendants in their Motion acknowledge not only the nationwide split of authority regarding the question presented, but the differing views among district courts in Michigan alone. See *Dana Ltd. v. American Axle and Mfg. Holdings, Inc.*, 2012 WL 2524008, *3 (W.D. Mich. June 29, 2012) ("There is a split in legal authority as to whether the CFAA applies when an employee, who has been granted access to his employer's computers, uses that access for an improper purpose."); *Experian Marketing Solutions, Inc. v. Lehman*, 2015 WL 5714541, *5 (W.D. Mich. Sept. 29, 2015) ("Experian cites a recent case from the Eastern District of Michigan in which the court held that the employer's policies were relevant to determining whether an employee had exceeded authorized access to company files."); and *Ajuba Intern., L.L.C. v. Saharia*, 871 F. Supp. 2d 671, 685 (E.D. Mich. May 14, 2012) ("The parties' dispute reflects a nationwide split of authority concerning the proper interpretation of the terms 'without authorization' and 'exceeds authorized access.'");.[1]

[1] See also *American Furukawa, Inc. v. Hossain*, 103 F. Supp. 3d 864, 876-77 (E.D. Mich. May 6, 2015) (emphasis in original) ("This Court will depart from the other district courts in Michigan that have found the Sixth Circuit favors a narrow approach to both the phrases 'without authorization' *and* 'exceeds authorized access.'") ("[T]his Court disagrees with the court decisions cited by

Yet Defendants' entire Motion simply ignores this divide. In fact, Defendants' Motion even ignores that these same district courts have also recognized the question presented by the Motion has *not* been resolved by the Sixth Circuit. Two of these district court decisions expressly noted the Sixth Circuit has not "squarely addressed" this situation, but rather (according to these courts) only indicated it would adopt a narrow view of the phrase "exceeds authorized access." See *Ajuba*, 871 F. Supp. 2d at 687 and *Dana*, 2012 WL 2524008 at 4 (both citing *Pulte Homes, Inc. v. Laborers' International Union of North America*, 648 F.3d 295 (6th Cir. 2011)). And the most recent district court decision relied upon by Defendants was blunter: "[t]he Sixth Circuit has not taken a position on this issue." *Experian*, 2015 WL 5714541 at 5 (discussing *Pulte*); see also *Hossain*, 103 F. Supp. 3d at 876 ("[T]he Sixth Circuit's opinion in *Pulte Homes* only adopted the 'narrow' approach as it pertained to interpreting the phrase 'without authorization;' not 'exceeds authorized access.'"). Defendants

---

Hossain that take a 'narrow' approach to the CFAA's 'exceeds authorized access' language in order to find that there can be no liability for an individual who violates a computer use policy."); *Dow Corning Corporation v. Chagnati*, 2015 WL 6735335 (E.D. Mich. Nov. 4, 2015) ("[I]ndividuals may also exceed authorized access by 'exceeding the purposes for which access is 'authorized'" because "material to potential liability under the statute is the scope of an individual's permissible access to information and the scope of an individual's ability to use that information."); and *Fabreeka International Holdings, Inc. v. Haley*, 2015 WL 7253019, *3 (E.D. Mich. Nov. 17, 2015) ("This Court has previously found that an employee could have exceeded authorized access when he allegedly violated a company policy that prohibited access of files with removable media without permission.").

nonetheless unequivocally assert "[t]he Sixth Circuit has adopted the 'narrow approach' in determining whether or not an employee *exceeds authorized access* for purposes of the CFAA." (See ECF Doc. No. 11, at p. 6) (discussing *Pulte*, *supra*) (italics in original) (underline added).[2]

In any event, Royal will address the nationwide split of authority concerning the phrase "exceeds authorized access" under the CFAA. First, Royal will discuss the differing approaches used by courts nationally for interpreting the phrase "exceeds authorized access" under the CFAA. Second, Royal will explain why the Sixth Circuit is likely to adopt, and this Court should follow, the broader approach taken by the First, Fifth, Seventh, Eighth, and Eleventh Circuits (and the *Hossain* court). Finally, Royal will describe how the allegations in the Complaint state claims for relief under the CFAA. Accordingly, the Motion should be denied.

[2] Defendants' disregard for applicable legal authority extends to the Local Rules as well. Defendants never sought concurrence before filing their Motion. See Local Rule 7.1(a)(1)(2). Nor did Defendants include a statement of the issues presented in their Motion, or identify the controlling or most appropriate authority for the relief sought. See Local Rule 7.1(d)(2). Defendants' Motion should be summarily denied. See *Steele v. Punch Bowl Detroit, LLC*, 2017 WL 2821970, *1-2 (E.D. Mich. June 29, 2017) (J. Cleland) ("This Court's practice guidelines, available online, state categorically that '[f]ailure to comply or to state the details of compliance as required may result in a denial of the motion without response.'") and *Zola H v. Snyder*, 2013 WL 5965615, at *1 (E.D. Mich. Nov. 8, 2013) (J. Cleland) ("A violation of this rule may result in a summary denial of the motion….").

LEGAL STANDARD

A motion to dismiss brought pursuant to Federal Rule of Civil Procedure 12(b)(6) tests the legal sufficiency of the complaint. *RMI Titanium Co. v. Westinghouse Elec. Corp.*, 78 F.3d 1125, 1134 (6th Cir. 1996). In ruling on such a motion, the Court must construe the complaint in a light most favorable to the plaintiff and accept all the factual allegations as true. *Tackett v. M & G Polymers, USA, LLC*, 561 F.3d 478, 488 (6th Cir. 2009). While the complaint does not need to contain "detailed factual allegations," it must contain more than "labels and conclusions" or "a formulaic recitation of the elements of a cause of action." *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 555 (2007). This means the complaint must contain sufficient factual matter that, when accepted as true, states a claim to relief that is plausible on its face. *Id*. at 570. A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged. *Id*. at 556. The plausibility standard, however, "'does not impose a probability requirement at the pleading stage; it simply calls for enough facts to raise a reasonable expectation that discovery will reveal evidence of illegal conduct.'" *Small v. City of Detroit*, 2017 WL 2418004, *1 (E.D. Mich. June 5, 2017) (quoting *Twombly*, 550 U.S. at 556).

ARGUMENT

I. This Court Should Deny The Motion Because Counts I And II State Claims Upon Which Relief Can Be Granted

Counts I and II of the Complaint state claims for violations of the CFAA. In pertinent part, an individual violates the CFAA when he or she either "[1] intentionally accesses a computer without authorization or [2] exceeds authorized access, and thereby obtains information from any protected computer." 18 U.S.C. § 1030(a)(2). While the statute does not define the phrase "without authorization," the statute does define the phrase "exceeds authorized access": "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6). The Complaint alleges Defendants exceeded authorized access to company owned computers and cellular phones by using them in violation of company policies. (See e.g., ECF Doc. 8, at p. ¶¶ 24; 29). The Complaint does not allege Defendants accessed company computers and cellular phones without authorization. (Id.). The question raised by the Motion is thus singular and limited: whether the Complaint sufficiently states claims that Defendants exceeded authorized access to company computers and cellular phones by using them in violation of company policies.

A. The Nationwide Split Of Authority

There is a "deep circuit split regarding interpretations and scope of the CFAA." *Hossain*, 103 F. Supp. 3d at 871. The *Ajuba* Court aptly summarized this divide:

> The split arises from cases in which an employer brings a CFAA claim against an employee who accesses the employer's computer to misappropriate confidential or proprietary business information to start a competing business venture or join a competitor. Courts around the country struggle with whether the CFAA applies in a situation where an employee who had been granted access to his employer's computers uses that access for an improper purpose. The split of authority specifically originates from competing interpretations of the terms "without authorization" and "exceeds authorized access," the statutory predicates for liability.

871 F. Supp. 2d at 685-86.

1. The "Broad" Approach

The split "has been cast as a clash between 'broad' and 'narrow' interpretations of the CFAA." *Hossain*, 103 F. Supp. 3d at 871. The First, Fifth, Seventh, Eighth, and Eleventh Circuits have all adopted a "broad" approach to interpreting and applying the phrase "exceeds authorized access." See *E.F. Cultural Travel BV, EF v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001); *International Airport Centers, L.L.C. v. Citrin*, 440 F.3d 418 (7th Cir. 2006); *U.S. v. John*, 597 F.3d 263 (5th Cir. 2010); *U.S. v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010); and *U.S. v. Teague*, 646 F.3d 1119 (8th Cir. 2011). These courts generally

hold that, even if an employee is granted access to information through a computer for some reasons, the employee may nonetheless exceed his authorized access under the CFAA by subsequently using his access to the information for prohibited or improper reasons. *Id*.

For example, in *Rodriguez*, the Eleventh Circuit affirmed the conviction of a Social Security Administration ("SSA") employee under the CFAA because he accessed information on a government computer in violation of a use restriction policy. 628 F.3d at 1260. As an employee of the SSA, the defendant was generally permitted to access certain governmental databases containing sensitive personal information about the general public. *Id*. In order to protect this information, however, the SSA implemented a policy that prohibited all employees from accessing these databases without a business reason. *Id*. The defendant refused to sign an acknowledgment form after receiving the policy, but he was nonetheless aware of the policy. *Id*. After it was discovered that, in an apparent effort to learn about multiple women the defendant was involved with, he had repeatedly accessed the database without a business reason, he was charged with, and convicted of, exceeding his authorized access to the information under the CFAA. *Id*. at 1261-62.

The defendant appealed. *Rodriguez*, 628 F.3d at 1263. In doing so, the defendant urged the Eleventh Circuit to follow the "narrow" approach to

interpreting the CFAA, which had been adopted by the Ninth Circuit one year earlier. *Id*. (citing *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009)). The Court declined:

> The Ninth Circuit held that *Brekka*, an employee of a residential addiction treatment center, had not violated the Act when he emailed documents that he was authorized to obtain to his personal email account. *Id*. at 1129. The treatment center argued that Brekka obtained the documents he emailed without authorization because he later used them for his own personal interests. *Id*. at 1132. The treatment center had no policy prohibiting employees from emailing company documents to personal email accounts, and there was no dispute that Brekka had been authorized to obtain the documents or to send the emails while he was employed. *Id*. at 1129. *Brekka* is distinguishable because the Administration told Rodriguez that he was not authorized to obtain personal information for nonbusiness reasons.

Id. In other words, while the Court distinguished *Brekka*, the Court also necessarily reasoned that (contrary to *Brekka*) an individual's right to access information for some reasons does not automatically preclude liability under the CFAA when the individual accesses information for prohibited reasons. *Id*. Rather, because a departmental policy informed the defendant he was not allowed to access the information for a "nonbusiness reason," the moment he "obtained personal information for a nonbusiness reason" he also "exceeded his authorized access and violated the [CFAA]." *Id*.

This is because, as the *Hossain* Court has reasoned, "an employee's 'authorized access' is completely dependent on the scope of the authorization provided by employers, who dictate at a threshold level how and what an employee may properly access, obtain, or alter on the employer's computer." 103 F. Supp. 3d at 879. This is "not an esoteric concept." *Id.* In fact, "the concept was originally advanced by the Ninth Circuit in *Brekka* when they acknowledged that 'the plain language of the statute dictates that 'authorization' depends on the *actions taken by the employer*.'" *Id*. at 879-80. (quoting *Brekka*, 581 F.3d at 1135) (emphasis in original).[3]

2. The "Narrow" Approach

The Second, Fourth, and Ninth Circuits have adopted the "narrow" approach to interpreting the phrase "exceeds authorized access." See *Brekka*, 581 F.3d

[3] See also *John*, 597 F.3d at 271-73 (employee of bank exceeded authorized access to customer account information database that she was generally permitted to access by sharing the information with non-employee in violation of company policy and furtherance of illegal scheme); *Teague*, 646 F.3d at 1121-23 (employee of government contractor exceeded authorized access to governmental student loan database that he was generally permitted to access by improperly accessing student-loan records of former United States president); *Explorica*, 247 F.3d at 582-584 (former employee of travel agency exceeded authorized access when he violated a confidentiality agreement by assisting a technology consultant hired by a competitor with developing a program that enabled the extraction of confidential pricing information from his former employer's website); and *Citrin*, 440 F.3d at 418-421 (former employee of real estate business violated CFAA when he erased files from computer before going into business for himself in violation of employment agreement because access to computer was revoked when he acquired interests adverse to his employer).

1127; *U.S. v. Nosal*, 676 F.3d 854 (9th Cir. 2011); *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012); and *U.S. v. Valle*, 807 F.3d 508 (2nd Cir. 2015). These courts generally hold that, once an employee is granted access to information through a computer for any reason, the employee is subsequently incapable of exceeding his authorized access under the CFAA, regardless of how he uses the information. *Id*.; see also *Ajuba*, 871 F. Supp. 2d at 686 and *Experian*, 2015 WL 5714541 at 5.

For example, in *Nosal*, the government indicted a former employee of an executive search firm for, among other things, violating the CFAA. 676 F.3d at 856. Shortly after leaving the company, the defendant persuaded some of his former colleagues – who remained employed by the company – to help him start a competing business. *Id*. The employees used their log-in credentials to download source lists, names, and contact information from a confidential database accessed through a company computer, and then transferred this information to the defendant. *Id*. While the employees were authorized to access the database containing the information, a company policy prohibited them from disclosing the information to the defendant. *Id*. After the government indicted the defendant for aiding and abetting the employees in exceeding their authorized access, the defendant moved to dismiss. *Id*. The district court eventually dismissed the CFAA counts. *Id*. The government appealed. *Id*.

The Ninth Circuit affirmed. *Nosal*, 676 F.3d at 864. In doing so, the Court initially acknowledged the competing approaches to interpreting the phrase "exceeds authorized access":

> This language can be read either of two ways: First, as [the defendant] suggests and the district court held, it could refer to someone who's authorized to access only certain data or files but accesses unauthorized data or files – what is colloquially known as "hacking." For example, assume an employee is permitted to access only product information on the company's computer but accesses customer data: He would "exceed authorized access" if he looks at the customer lists. Second, as the government proposes, the language could refer to someone who has unrestricted physical access to a computer, but is limited in the use to which he can put the information. For example, an employee may be authorized to access customer lists in order to do his job but not to send them to a competitor.

Id. at 856-57.

"While the CFAA is susceptible to the government's broad interpretation," the Court continued, "we find [the defendant's] narrower one more plausible." *Nosal*, 676 F.3d at 858. This is because, the Court suggested, the broader approach "would transform the CFAA from an anti-hacking statute into an expansive misappropriation statute." *Id.* at 857. According to the Court:

> The government agrees that the CFAA was concerned with hacking, which is why it also prohibits accessing a computer "without authorization." According to the government, *that* prohibition applies to hackers, so the "exceeds authorized access" prohibition must apply to people who are authorized to use the computer, but do so

> for an unauthorized purpose. But it is possible to read both prohibitions as applying to hackers: "[W]ithout authorization" would apply to *outside* hackers (individuals who have no authorized access to the computer at all) and "exceeds authorized access" would apply to *inside* hackers (individuals whose initial access to a computer is authorized but who access unauthorized information or files). This is a perfectly plausible construction of the statutory language that maintains the CFAA's focus on hacking rather than turning it into a sweeping Internet-policing mandate.

Id. at 858 (italics in original).

In short, the Ninth Circuit concluded, the decisions from the circuits applying the "broad" approach have "failed to consider the effect on millions of ordinary citizens caused by the statute's unitary definition of "exceeds authorized access" and "failed to apply the long-standing principle that we must construe ambiguous criminal statutes narrowly so as to avoid making criminal law in Congress's stead." *Nosal*, 676 F.3d at 862-63 (internal citations and quotations removed).[4]

[4] See also *WEC*, 687 F.3d at 204 (employee did not exceed authorized access to computer when he downloaded confidential information in violation of company policy and subsequently used the information to assist a competitor because defendant was generally allowed to access the information) and *Valle*, 807 F.3d at 508 (former police officer did not exceed authorized access to confidential police database when he searched for an individual's personal information in violation of a policy prohibiting him from using the database without a law enforcement purpose because he was generally allowed to access the database).

B. The Sixth Circuit Is Likely To Adopt, And This Court Should Follow, The "Broad" Approach

The Sixth Circuit has discussed the phrases "without authorization" and "exceeds authorized access" only once. See *Pulte*, 648 F.3d at 303-04. In *Pulte*, a plaintiff home builder commenced an action against a national labor union and two of its officers alleging, among other things, violations of the CFAA. *Id*. at 299. The plaintiff alleged that, because of a dispute regarding the dismissal of an employee, defendants hired an auto-dialing service, and encouraged their members, to bombard plaintiff's sales offices and three of its executives with thousands of phone calls and emails. *Id*. at 298-99. Plaintiff further alleged the extreme volume of communications succeeded in frustrating access to the plaintiff's voicemail system, preventing customers from reaching its sales offices, and forced one employee to shut down her cellular phone. *Id*. Defendants moved to dismiss. *Id*. at 299. After the district court dismissed the action, plaintiff appealed. *Id*.

The Sixth Circuit affirmed dismissal of the "access claim." *Pulte*, 648 F.3d at 303. In doing so, the Court first noted it did not need to determine whether the communications had "accessed" Pulte's computers because, even if they had, Pulte had failed to sufficiently allege access "without authorization." *Id*. Notwithstanding "some similarities" in the phrases "without authorization" and "exceeds authorized access," the Court continued, it "must, if possible, give

meaning to both prohibitions." *Id*. at 304. "Because Congress," the Court explained, "left the interpretation of 'without authorization' to the courts," the Court should "start with ordinary usage." *Id*. at 303. Given that the "plain meaning of 'authorization' is 'the conferment of legality; sanction,'" the Court reasoned, "a defendant who accesses a computer 'without authorization' does so without sanction or permission.'" *Id*. at 303-04 (citing 7 Oxford English Dictionary at 696, 798 (2d ed.1989)). According to the Court, however:

> Unlike the phrase "without authorization," the CFAA helpfully defines "exceeds authorized access" as "accessing a computer with authorization and using such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." Under this definition, "an individual who is authorized to use a computer for certain purposes *but goes beyond those limitations* ... has 'exceeded authorized access.'" [quoting *Brekka*, *supra*]. In contrast, "a person who uses a computer 'without authorization' *has no rights, limited or otherwise*, to access the computer in question." *Id.*

Id. at 304. (emphasis in original) (internal quotations and citations removed).

The Court then posited and answered the question presented: "whether [defendant] had *any* right to call [plaintiff's] offices and email its executives" – "[i]t did. 648 F.3d at 304 (emphasis in original). This is because, the Court explained, plaintiff's telephones and email system were generally open to the public. *Id*. According to the Court, while plaintiff complained about the extreme volume and manner of the communications, there was no allegation any of them

were somehow unauthorized. *Id*. In the Court's view, plaintiff's "complaint thus amounts – at most – to an [unpled][5] allegation that [defendant] exceeded its authorized access." *Id*.

1. The *Pulte* Decision Strongly Indicates The Sixth Circuit Will Adopt The "Broad" Approach To Interpreting The Phrase "Exceeds Authorized Access"

The *Pulte* Court found that CFAA access claims encompass two separate "prohibitions," which each have distinct meanings. 648 F.3d at 304. The "distinction is important." *Hossain*, 103 F. Supp. 3d at 876. This is because, unlike the Sixth Circuit's treatment of the phrase "without authorization," "with respect to the phrase 'exceeds authorized access,' the Sixth Circuit did not go beyond the plain language of the CFAA's provided language." *Id*. at 877. The Sixth Circuit instead cited the Ninth Circuit's statement in *Brekka* to describe the CFAA's definition of "exceeds authorized access." *Id*.

In doing so, the Sixth Circuit *emphasized* that, unlike the phrase "without authorization," when a person violates this portion of the CFAA, the person has authorization to use a computer "'for certain purposes, *but goes beyond those limitations*.'" *Hossain*, 103 F. Supp. 3d at 877 (quoting *Pulte*, *supra*; quoting *Brekka*) (emphasis in original). While the Court was not confronted with

[5] See *Pulte Homes, Inc., v. Laborers' International Union of North America, et al.*, 2009 WL 4896964 (E.D. Mich.) (First Amended Verified Complaint, ¶¶ 61-68) (no allegation defendant exceeded authorized access).

addressing the split of authority concerning "exceeds authorized access," the emphasized words nonetheless provide a compelling indication the Sixth Circuit favors the "broad" approach. Indeed, the Sixth Circuit's emphasis recognizes that merely because someone is granted authorization to access information for "certain purposes" (i.e, for business reasons) that person exceeds his authorized access when he "goes beyond those limitations" (i.e., accesses the information for nonbusiness reasons). *Pulte*, 648 F.3d at 304; see also *Hossain*, 103 F. Supp. 3d at 879 ("[S]omeone exceeds authorized access by obtaining information in a prohibited manner, even if the accesser might be entitled to obtain the same information under other circumstances.").

Moreover, the Sixth Circuit's explanation of the phrase "exceeds authorized access" does not comport with the purported logic of the "narrow" approach. For example, in *Nosal*, the Ninth Circuit completely rejected liability under the CFAA for anyone granted initial access to information that later uses it improperly, yet reasoned that "an employer is certainly able to bring an action against an individual under the CFAA if the individual accesses the employer's computers in a manner that exceeds 'security measures.'" *Hossain*, 103 F. Supp. 3d at 879 (citing *Nosal*, 676 F.3d at 858). As the *Hossain* Court reasoned, however, the *Nosal* Court's hypothetical offers more of a distinction without a difference than a meaningful illustration:

> This Court fails to see a difference between an employee who circumvents "security measures," and an employee who circumvents explicit computer limitations provided by an employer for employees regarding the employee's access, use, or purpose when accessing the employer's systems. To this Court, such explicit policies are nothing but "security measures" employers may implement to prevent individuals from doing things in an improper manner on the employer's computer systems.

Id. Accordingly, the *Pulte* Decision strongly indicates the Sixth Circuit will adopt, and this Court should follow, the "broad" approach to interpreting the phrase "exceeds authorized access" under the CFAA.

2. The Sixth Circuit Is Likely To Give Deference To The Supreme Court's Discussion Of The CFAA In *Musacchio*

The Supreme Court has not resolved the nationwide split of authority concerning how to interpret the CFAA. This is not because the Court is unfamiliar with the divide. See e.g., *Rodriguez v. U.S.*, 563 U.S. 966 (2011) (certiorari denied); *John v. U.S.*, 568 U.S. 1163 (2013) (certiorari denied) and *WEC Carolina Energy Sols. LLC v. Miller*, 568 U.S. 1079 (2013) (certiorari dismissed). Less than two years ago, however, the Court did discuss how someone may violate the relevant portion of CFAA, albeit in another context. See *Mussachio v. U.S.*, 136 S. Ct. 709, 713 (2016). In *Musacchio*, the defendant was convicted of accessing a competitor's computer system without authorization when his competitor's former employee (his new colleague) provided him password access to the system. *Id*. At trial, the district court mistakenly

instructed the jury that violating the CFAA required the government to prove the defendant had accessed a computer *both* "without authorization *and* exceed[ed] authorized access." *Id*. at 714 (emphasis in original). The parties agreed the instruction was erroneous because it added an additional element for proving a violation of the CFAA. *Id*. Despite the error, the Court affirmed the conviction. *Id*.

Significantly, in doing so, the Court described its understanding of how someone may violate the CFAA. According to the Court, the "statute thus provides two ways of committing the crime of improperly accessing a protected computer: (1) obtaining access without authorization; and (2) obtaining access with authorization *but then using that access improperly*." *Musacchio*, 136 S.Ct. at 713 (citing 18 U.S.C. § 1030(a)(6)) (emphasis added). While this passage alone may not definitely resolve the circuit split, the Sixth Circuit is nonetheless likely to give deference to the *Musacchio* Court's discussion of the CFAA.

First, while the *Musacchio* Court was not squarely addressing the same question presented in this case, its description of the CFAA was at least important, if not necessary, to the decision. This is because the Court could not acknowledge it was error to require proof of both "without authorization" and "exceeds authorized access" without recognizing there are separate ways someone can violate the CFAA. Second, even if the language is merely dicta,

"lower courts are obligated to follow Supreme Court dicta, particularly where there is not substantial reason for disregarding it, such as age or subsequent statements undermining its rationale." *In re Baker*, 791 F.3d 677, 682 (6th Cir. 2015). As one court in the Eastern District has explained:

> [I]t must be remembered that even dictum is entitled to serious consideration by the lower federal courts when it appears in an opinion by the Supreme Court. Since docket constraints do not permit the Supreme Court to pass upon all issues of federal law that arise within the system, the Court frequently paints with a brush somewhat broader than necessary to decide the case immediately before it in order that general guidance may be provided to the courts below.

Matter of Comac Co., 402 F. Supp. 43, 45 (E.D. Mich. Oct. 15, 1975).

This is likely the situation here. The *Musacchio* Court was undoubtedly aware of the circuit split concerning the phrase "exceeds authorized access" before it issued the opinion. Indeed, aside from the multiple petitions for certiorari in other cases (cited above), the defendant expressly discussed, and invited the Court to address, the circuit split in both his petition for certiorari and brief on appeal. See *Musacchio v. United States of America*, 2015 WL 1064743, *20, Fn. 5 (U.S. 2015) and *Musacchio v. United States of America*, 2015 WL 5138667, *6, 11-12 (U.S. 2015). While the Court declined to directly confront the split, the Court *did* do something else. To wit: instead of merely quoting the statutory language and emphasizing the "or" (which the Court initially did), the Court also included a

second sentence elaborating upon how the CFAA can be violated by using some of the same (or very similar) language lower courts have used to describe the split: "but then using that access improperly." *Musacchio*, 136 S.Ct. at 713 (underline added).[6] It is thus reasonable to infer the *Musacchio* Court was "paint[ing] with a brush somewhat broader than necessary to decide the case immediately before it in order that general guidance may be provided to the courts below." *Matter of Comac Co.*, 402 F. Supp. at 45. Accordingly, the Sixth Circuit is likely to give deference to the Supreme Court's discussion of the CFAA in *Musacchio*.

C. Counts I And II Of The Complaint Properly State Claims That Defendants Violated The CFAA When They Exceeded Their Authorized Access To Company Owned Computers And Cellular Phones By Using Them In Violation Of Company Policies

In order to state a violation of the CFAA, Royal must plead: (1) that Defendants intentionally accessed a computer (2) without authorization or by exceeding authorized access; and (3) that Defendants thereby obtained information (4) from the protected computer; and (5) there was loss to one or more persons during any one-year period aggregating at least $5,000 in value. See *Hossain*, 103 F. Supp. 3d at 870. Defendants' Motion claims the Complaint

[6] See e.g., *WEC*, *supra* ("uses his access for a purpose contrary to the employer's interests"); *Valle*, *supra* ("with an improper purpose, he accesses"); *Ajuba*, *supra* ("uses that access for an improper purpose"); *Dana*, *supra* ("uses that access for an improper purpose"); *John*, *supra*, ("exceeding the purposes for which access is 'authorized'"); *Pulte*, *supra* ("for certain purposes but goes beyond those limitations"); and *Nosal*, *supra* ("but do so for an unauthorized purpose").

fails to allege only one of these elements: that Defendants exceeded their authorized access. Defendants are wrong. As discussed above, the Sixth Circuit is likely to adopt, and this Court should follow, the "broad" approach to interpreting the phrase "exceeds authorized access." In accordance with the "broad" approach, employers may "dictate at a threshold level how and what an employee may properly access, obtain, or alter on the employer's computer." *Hossain*, 103 F. Supp. 3d at 879. The Complaint alleges Royal did precisely this.

Royal promulgated an Employee Handbook and GPS Tracking Policy (collectively "Policies"). (See ECF Doc. No. 8, ¶¶ 13-18). Defendants were aware of, and familiar with, the Policies. (Id. at ¶¶ 13-15, 18). The Policies defined and limited Defendants' rights to use their company computers and cellular phones. (Id. at ¶¶ 13-18). Among other things, the Policies prohibit impairing or altering company property (¶ 16 b.); require employees to maintain data stored on computer equipment (¶ 16 e.); prohibit the use of company equipment and property for personal activities (¶ 16 e.); admonish employees that electronic information systems are to be used for company business only (¶ 16 j.); admonish employees that company hardware (computers and phones) and software (computer files and the e-mail system) are company property intended for business use (¶ 16 k.); admonish employees that equipment, services, and technology provided to access the internet remain at all times the property of the

company (¶ 16 l.); admonish employees that cellular phones are intended to be used for business purposes (¶ 16 n.); admonish employees that sending or posting trade secrets, or proprietary information, outside of the organization is considered prohibited abuse of the internet access provided by the company (¶ 16 m.); and prohibit employees from disabling or interfering with any functions, or removing any software, functions, or apps at any time, on a company issued cellular phone (¶ 18).

In fact, the Policies also include an "Information Security/Confidentiality" section, which reminds employees they "have been entrusted with one of [Royal's] most valuable assets – information – and they have a responsibility to protect it and see that it is used only for its intended business purpose" because Royal "use[s] information on a daily basis that could be useful to competitors…" (See ECF Doc. No. 8, ¶ 17). The section also admonishes employees that confidential information includes, among other things, computer records, word processing documents, paper reports, electronic data storage, employment records, and client information. (Id.). And the section directs employees not to disclose to anyone outside the company any business-related information that has not been disclosed to the public. (Id.). Significantly, the Policies even warn employees that "[a]ny unauthorized use, retention or disclosure of any [Royal]

resources or property will be regarded as theft … and may prompt various civil and/or criminal legal actions." (¶ 16 g.).

Nevertheless, and despite these clear and known company policies, the allegations of the Complaint establish Defendants exceeded their authorized access to their computers and cellular phones. First, after Mike had already accepted employment from Royal's competitor (unbeknownst to Royal), but while still employed and using time off ostensibly for a "personal family emergency," Mike: (a) forwarded two quotes generated for Royal customers to his personal email account; (b) forwarded confidential payroll records for two Royal employees to his personal email account; (c) and destroyed all data on his company provided computer. (See ECF Doc. No. 8, ¶ 21, 24). Second, after Kelly had already accepted employment from Royal's competitor (unbeknownst to Royal), but while still employed by Royal, Kelly: (a) emailed a "Salesperson Summary Report" to Mike's personal email account, which contained confidential information concerning revenue, profits, and other details relating to eight of the salespeople in Royal's Parts Division; (b) forwarded a sales inquiry to her personal email account that contained customer pricing information and had been allocated to Kelly by her manager for the purpose of soliciting the customer on behalf of Royal; and (c) destroyed all data on her company provided cellular phone. (See ECF Doc. No. 8, ¶ 21, 29).

Defendants' actions violated the Policies identified above. *Among other things*, Defendants' used their access to company information through Royal's computers and cellular phones to obtain sensitive and confidential company information, which they surreptitiously transferred to Mike's personal email account for obviously nonbusiness reasons designed to benefit only Defendants' personal, and their new employer's (Royal's competitor's), interests.[7] Moreover, even standing alone, Mike's destruction of the data on his computer, and Kelly's destruction of the data on her cellular phone, were per se violations of the Policies. (See e.g., ECF Doc. No. 8, ¶¶ 16 b.; 16 e.; 18). Accordingly, Counts I and II of the Complaint properly state claims for violations of the CFAA.

WHEREFORE, Plaintiff Royal Truck & Trailer Sales and Service, Inc. respectfully requests that, in accordance with Federal Rule of Civil Procedure 12, this Court deny Defendants Mike Kraft's and Kelly Matthews a/k/a Kelly Schlimmer's Motion to Dismiss Under Rule 12(b)(6) for Failure to State a Claim and Under Rule 12(b)(1) for Want of Subject Matter Jurisdiction.

Respectfully submitted,
KOTZ SANGSTER WYSOCKI P.C.

Dated: May 8, 2018 By: /s/ Anthony M. Sciara

[7] In fact, one of the quotes Mike absconded with was for Royal customer, Ryder Truck, which is the same customer relationship giving rise to Mike's breach of his duty of loyalty and tortious interference. (See ECF Doc. No. 8, ¶¶ 48-59).

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

ROYAL TRUCK & TRAILER SALES AND SERVICE, INC.,
Plaintiff,

v.

MIKE KRAFT; and KELLY MATTHEWS A/K/A/ KELLY SCHLIMMER,
Defendants.

Case No. 3:18-cv-10986-RHC-EAS
Hon. Robert H. Cleland
Mag. Elizabeth A. Stafford

KOTZ SANGSTER WYSOCKI P.C.
By: Anthony M. Sciara (P75778)
Christopher A. Ferlito (P80574)
Counsel for Royal Truck & Trailer
400 Renaissance Center
Suite 3400
Detroit, Michigan 48243
313-259-8300
asciara@kotzsangster.com
cferlito@kotzsangster.com

VARNUM LLP
By: Richard T. Hewlett (P41271)
Salvatore J. Vitale (P75449)
Counsel for Kraft and Matthews
39500 High Pointe Boulevard
Suite 350
Novi, Michigan 48375
248-567-7400
rthewlett@varnumlaw.com
sjvitale@varnumlaw.com

CERTIFICATE OF SERVICE

I hereby certify that, to the best of my information, knowledge, and belief, and on the 8th day of May, 2018, I electronically filed the foregoing pleadings with the Clerk of the Court using the ECF system, which will send notification of, and serve, such filing to all counsel of record.

/s/ Lindsey Pfund